数理解析研究所講究録
1057 巻 1998 年 38-40

On the number of crossed homomorphisms from a finite cyclic p-group to a finite p-group

Yugen Takegahara
竹ヶ原 裕元
Muroran Institute of Technology
室蘭工業大学

For finite groups H and C such that C acts on H, let $\mathcal{Z}(C,H)$ denote the set consisting of all complements of H in the semidirect product CH with respect to a fixed action of C on H, i.e.,

$$\mathcal{Z}(C,H)=\{D\leq CH|D\cap H=\{1\},DH=CH\},$$

which bijectively corresponds to the set of all crossed homomorphisms from C to H([5, Ch.2,§8]), and let $z(C,H)=\sharp\mathcal{Z}(C,H)$. One of the famous result concerning this number is the theorem due to P. Hall ([4, Theorem 1.6]):

For a finite group H and for an automorphism θ of H such that $\theta^n=1$, the number of elements x of H that satisfy the equation

$$(x\theta^{-1})^n=x\cdot x^{\theta}\cdot x^{\theta^2}\cdots x^{\theta^{n-1}}=1$$

is a multiple of $\gcd(n,|H|)$.

This result is a generalization of the theorem of Frobenius:

The number of solutions of $x^n=1$ in a finite group H is a multiple of $\gcd(n,|H|)$.

Let p denotes a prime integer. We shall show some results about $z(C,H)$ where C and H are p-groups. For a finite group G, let $C_2(G)=[G,G]$, and define $C_i(G)=[C_{i-1},G]$ for each integer i such that $i\geq 3$. We use the following famous theorem due to P.Hall.

Theorem 1 ([3, 6]) *Let x and y be any elements of a finite group G. Then there exist elements $c_2,c_3,\ldots,c_n$ of $<x,y>$ such that c_i is an element of $C_i(<x,y>)$ for each i and that*

$$x^ny^n=(xy)^nc_2^{e_2}c_3^{e_3}\cdots c_n^{e_n}$$

where $e_i=n(n-1)\cdots(n-i+1)/i!$ for each i.

Using Theorem 1, we obtain the following.

Proposition 1 *Let G be a finite p-group, and let c be an element of G. Assume that* $\exp C_i(G) \leq p^{u-i+2}$ *for each integer i such that $i \geq 2$. If either $p > 2$ or* $\exp C_2(G) \leq p^{u-1}$, *then $(cx)^{p^u} = c^{p^u}$ for any element x of G such that $x^{p^u} = 1$.*

Let H be a finite p-group that is not $\{1\}$, and let C be a finite cyclic group of order p^u that acts on H. Let $C_1(CH) = H$. Clearly, $C_{i+1}(CH) \subset C_i(CH)$ for each positive integer i. By [6, p.43,Corollary 2], $C_2(CH) \neq C_1(CH)$. It follows that $C_{i+1}(CH) \neq C_i(CH)$ for each positive integer i, provided $C_i(CH) \neq \{1\}$([6]). Let j be the least integer such that $|C_{j+1}(CH)| \leq p^{u-1}$, and let $Q(CH)$ be a normal subgroup of CH defined by

$$Q(CH) = \Omega_u(C_j(CH)).$$

Then $|Q(CH)| \geq \gcd(p^u, |H|)$, and $|[Q(CH), CH]| \leq p^{u-1}$. Furthermore,

$$\exp Q(CH) \leq p^u$$

by Proposition 1. The following proposition is a consequence of Proposition 1.

Proposition 2 *Let H be a finite p-group, and let C be a cyclic p-group that acts on H. Then* $z(C, H) \equiv 0 \bmod |Q(CH)|$.

Corollary 1 ([2, Proposition 3.3]) *Let H be a finite p-group, and let C be a cyclic p-group that acts on H. Then* $z(C, H) \equiv 0 \bmod \gcd(|C|, |H|)$.

By using Propositions 1 and 2, we get the following.

Theorem 2 *Let H be a finite p-group, and let C be a cyclic group of order p^u that acts on H. Assume that H contains no cyclic normal C-invariant subgroup of order p^{u+1}. If either $p > 2$ or H contains no proper cyclic normal C-invariant subgroup of order p^u, then* $z(C, H) \equiv 0 \bmod \gcd(p^{u+1}, |H|)$.

Equivalently, the following theorem holds.

Theorem 3 *Let H be a finite p-group, and let θ be an automorphism of H such that $\theta^{p^u} = 1$. Assume that H contains no cyclic normal subgroup Q of order p^{u+1} such that $Q^\theta = Q$. If either $p > 2$ or H contains no proper cyclic normal subgroup Q of order p^u such that $Q^\theta = Q$, then the number of elements x of H that satisfy the equation*

$$(x\theta^{-1})^{p^u} = x \cdot x^\theta \cdot x^{\theta^2} \cdots x^{\theta^{p^u-1}} = 1$$

is a multiple of $\gcd(p^{u+1}, |H|)$.

Corollary 2 *Let H be a finite p-group that contains no normal cyclic subgroup of order p^{u+1}. If either $p > 2$ or H contains no proper cyclic normal subgroup of order p^u, then the number of solutions of $x^{p^u} = 1$ in H is a multiple of* $\gcd(p^{u+1}, |H|)$.

We also have some results in the case where C is an abelian p-group that acts on a p-group H. The following theorem is a result concerning to the number of cocycles.

Theorem 4 ([1]) *Let H and C be finite abelian p-groups such that C acts on H. Then* $z(C,H) \equiv 0 \bmod \gcd(|C|,|H|)$.

Sketch of proof. Suppose that $C = C_1 \times C_2 \times \cdots \times C_r$, where $C_1, C_2, \ldots, C_r$ are cyclic p-groups. Let x_j be a generator of C_j for each j. Let G_i denote the set of all elements h of H such that $[h, x_j] = 1$ for any j except i. Assume that $|G_i| \geq |C_i|$ for any i. Let $G = Q(C_1G_1) \times \cdots \times Q(C_rG_r)$. Then $|G| \geq |C|$. For each i, if the order of element y of C_iH is $|C_i|$, then the order of yh is also $|C_i|$ for any element h of $Q(C_iG_i)$ by Proposition 1. Thereby, G acts on $\mathcal{Z}(C,H)$, and the action is semiregular. Hence, $z(C,H) \equiv 0 \bmod |C|$. Next, assume that $|G_{i_0}| < |C_{i_0}|$ for some i_0. By Corollary 1, G_{i_0} acts on $\mathcal{Z}(C_{i_0}, H)$. Moreover, $H/C_H(C)$ acts on $\mathcal{Z}(C,H)$ by conjugation. So, the action of $H/C_H(C) \times G_{i_0}$ on $\mathcal{Z}(C,H)$ is naturally defined. We have that the order of the stabilizer of an element of $\mathcal{Z}(C,H)$ is $|G_{i_0} : C_H(C)|$. Hence, $z(C,H) \equiv 0 \bmod |H|$. Thus, the theorem holds. □

It follows from [2, Proposition 3.2] that if an elementary abelian p-group C acts on a finite p-group H, $z(C,H) \equiv 0 \bmod |C|$. The following proposition is a generalization of Corollary 1.

Proposition 3 ([1]) *Let H be a finite p-group, and let C be a finite abelian p-group that acts on H. Assume that C is the direct product of a cyclic p-group and an elementary abelian p-group. Then* $z(C,H) \equiv 0 \bmod \gcd(|C|,|H|)$.

This results yields the following.

Theorem 5 ([1, 2]) *Let A be a finite group such that a Sylow p-group of A/A' is the direct product of a cyclic p-group and an elementary abelian p-group. For any finite group G, the number of homomorphisms from A to G is a multiple of* $\gcd(|A/A'|_p, |G|)$, *where $|A/A'|_p$ is the highest power of p dividing $|A/A'|$.*

References

[1] T. Asai and Y. Takegahara, On the number of crossed homomorphisms, preprint.

[2] T. Asai and T. Yoshida, $|\mathrm{Hom}(A,G)|$, II, *J. Algebra*, **160** (1993), 273–285.

[3] P. Hall, A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.*(2), **36** (1933), 29–95.

[4] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.*(2), **40** (1935), 468–501.

[5] M. Suzuki, Group Theory I, Springer–Verlag, New York, 1982.

[6] M. Suzuki, Group Theory II, Springer–Verlag, New York, 1986.